



(43) Internationales Veröffentlichungsdatum
17. Februar 2005 (17.02.2005)

PCT

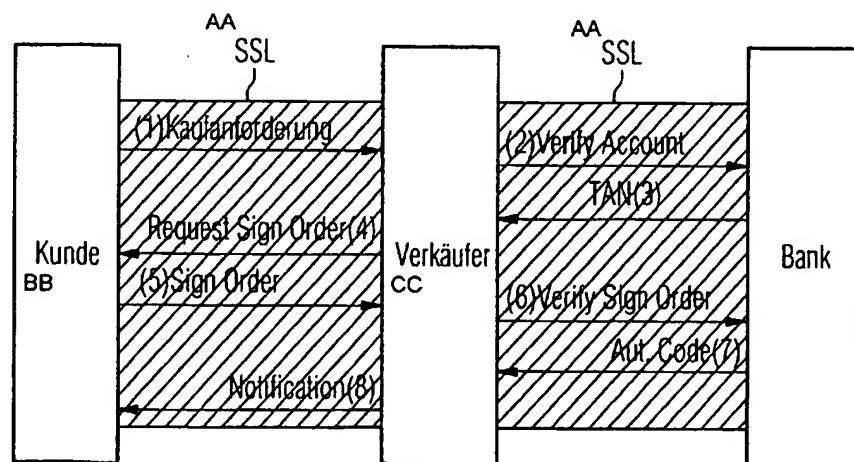
(10) Internationale Veröffentlichungsnummer
WO 2005/015514 A1

- | | |
|---|---|
| <p>(51) Internationale Patentklassifikation⁷: G07F 19/00,
7/10, G06F 17/60, H04L 29/06</p> <p>(21) Internationales Aktenzeichen: PCT/EP2004/051749</p> <p>(22) Internationales Anmeldedatum:
9. August 2004 (09.08.2004)</p> <p>(25) Einreichungssprache: Deutsch</p> <p>(26) Veröffentlichungssprache: Deutsch</p> <p>(30) Angaben zur Priorität:
103 36 805.1 11. August 2003 (11.08.2003) DE</p> <p>(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): SIEMENS AKTIENGESELLSCHAFT [DE/DE];
Wittelsbacherplatz 2, 80333 München (DE).</p> <p>(72) Erfinder; und</p> <p>(75) Erfinder/Anmelder (nur für US): REXHA, Blerim
[AL/AT]; Favoritenstrasse 33/2/16, A-1040 Wien (AT).</p> | <p>TREYTL, Albert [AT/AT]; Gusshausstrasse 27-29/384,
A-1040 Wien (AT).</p> <p>(74) Gemeinsamer Vertreter: SIEMENS AKTIENGE
SELLSCHAFT; Postfach 22 16 34, 80506 München
(DE).</p> <p>(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.</p> <p>(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,</p> |
|---|---|

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR TRANSMITTING PROTECTED INFORMATION TO SEVERAL RECEIVERS

(54) Bezeichnung: VERFAHREN ZUM ÜBERMITTELN VON GESCHÜTZTEN INFORMATIONEN AN MEHRERE EMPFÄNGER



AA...PURCHASE REQUEST
BB...CUSTOMER
CC...PURCHASER

(57) Abstract: The invention relates to first information which is determined for a first receiver. Said first information is transmitted together with secondary information, which is determined for a second receiver in a common information unit to the first receiver. The first information can be encrypted according to specifications of the first receiver. The secondary information, which can be made of several components, is encrypted according to the specifications of the second receiver, for example, with an open key, a so-called public key. Said public key encryption methods have various embodiments and security steps. Said methods ensure that the first receiver, upon receipt of the complete information, can not encrypt pieces of information therefor not intended therefor.

[Fortsetzung auf der nächsten Seite]

BEST AVAILABLE COPY

WO 2005/015514 A1



GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht

— vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

BEST AVAILABLE COPY

(57) Zusammenfassung: Erste Informationen, die für einen ersten Empfänger bestimmt sind, werden zusammen mit zweiten Informationen, welche für einen zweiten Empfänger bestimmt sind, in einer gemeinsamen Informationseinheit an den ersten Empfänger versendet. Die ersten Informationen können dabei gemäss den Vorgaben des ersten Empfängers verschlüsselt sein. Die zweiten Informationen, welche aus mehreren Bestandteilen bestehen können, werden gemäss den Vorgaben des zweiten Empfängers verschlüsselt, beispielsweise mit einem öffentlichen Schlüssel, einem sogenannten "public key". Diese "public key" Verschlüsselungsverfahren sind bereits in verschiedenen Ausführungen und Sicherheitsstufen bekannt. Durch dieses Vorgehen wird gewährleistet, dass der erste Empfänger bei Erhalt der kompletten Information die für ihn nicht bestimmten Informationsanteile nicht entschlüsseln kann.